UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/749,412	01/02/2004	Ryo Ochi	247305US6	2841

22850   7590   08/19/2009
OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, L.L.P.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER
LE, CANH

ART UNIT	PAPER NUMBER
2439	

NOTIFICATION DATE	DELIVERY MODE
08/19/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

	Application No.	Applicant(s)
	10/749,412	OCHI ET AL.
Office Action Summary	Examiner	Art Unit	
	CANH LE	2439	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS,
WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>21 May 2009</u>.
2a) ☐ This action is **FINAL**.   2b) ☒ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
    closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>1-6,8-16 and 18-22</u> is/are pending in the application.
     4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) <u>1-6,8-16 and 18-22</u> is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☒ The specification is objected to by the Examiner.
10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
     Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
     Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
     a) ☐ All b) ☐ Some * c) ☐ None of:
       1. ☐ Certified copies of the priority documents have been received.
       2. ☐ Certified copies of the priority documents have been received in Application No. _____.
       3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
          application from the International Bureau (PCT Rule 17.2(a)).
     * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
     Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
     Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in

37 CFR 1.17(e), was filed in this application after final rejection. Since this application is

eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e)

has been timely paid, the finality of the previous Office action has been withdrawn pursuant to

37 CFR 1.114. Applicant's submission filed on 05/21/2009 has been entered.

This Office Action is in response to the communication filed on 05/21/2009.

Claims 7 and 17 have been cancelled.

Claims 1, 9, 11, 19, 21, and 22 have been amended.

Claims 1-6, 8-16, and 18-22 have been examined and are pending.

Response to Amendment

Applicant's arguments with respect to claims 1-6, 8-16, and 18-22 have been considered but are

moot in view of the new ground(s) of rejection.

Claim Objections

Claims 2-6, 10, 12-16, 18, and 20 are objected to because of the following informalities:

Appropriate correction is required.

(Claims 2-6, 10; line 1): "An encryption processing" should be replaced by "The

encryption processing" to avoid potentially antecedent basis.

(Claims 12-16, 18; line 1): "An encryption processing" should be replaced by "The

encryption processing" to avoid potentially antecedent basis.

(Claim 20, line 1): "An encryption processing" should be replaced by "The encryption

processing" to avoid potentially antecedent basis.

Specification

The specification is objected to as failing to provide proper antecedent basis for the

claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the

following is required: Claims 1, 9, 11, 19, and 21-22 recite the limitation "***by inserting at least***

one encryption processing unit from one of the groups between encryption processing units

from another one of the groups so that performance of at least ***one encryption processing unit***

from one of the group is performed at a time between ***performance of encryption processing***

units from another one of the groups." (emphasis added). However, the aforementioned

limitation is not found in the specification. There is insufficient antecedent basis for this

limitation.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-6, 8-16, and 18-22 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claims 1, 9, 11, 19, and 21-22 recite the limitation "**_by inserting at least one encryption processing unit from one of the groups between encryption processing units from another one of the groups_** so that performance of at least **_one encryption processing unit_** from one of the group is performed at a time between **_performance of encryption processing units_** from another one of the groups." (emphasis added). However, the aforementioned limitations are not discussed in the specification. Although the Applicant points out that *"the changes and additions to the claims are not supported by the originally filed specification on page 30, line 5 to page 31, line 12 and figs 6-8."* However, this does not imply "**_inserting at least one encryption processing unit_** from **_one of the groups between encryption processing units from another one of the groups_**". The Examiner respectfully requests the Applicant point out where in the specification support can be found for the aforementioned newly added limitations. Applicant is required to cancel the new matter in the reply to this Office Action.

Claims 2-6, 8, 10, 12-16, 18, and 20 are dependent on either claims 1, 9, 11, or 19, and therefore inherit the 35 U.S.C 112, first paragraph as failing to comply the written description requirement of the independent claims.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and
distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1-6, 8-16, and 18-22 are rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention.

Claims 1, 9, 11, 19, and 21-22 recite the limitation "where the input data to be encrypted

__for one of the groups is different__ and generated independently relative to the input data to be

encrypted for another one of the groups" (emphasis added).   It is unclear as to what data *the*

input data to be encrypted for one of the groups is different.

Claims 1, 9, 11, 19, and 21-22 recite the limitation "*__by inserting at least one encryption__*

__processing unit from one of the groups between encryption processing units from another one__

__of the groups__ so that performance of at least *__one encryption processing unit__* from one of the

group is performed at a time between *__performance of encryption processing units__* from another

one of the groups." (emphasis added). The phrases are not discussed in the specification, and

therefore the aforementioned phrases are vague in reference to what of "inserting at least one

encryption processing unit encryption" in the between the groups.

Claim 8 recites the limitation "to be *__capable of__* identifying which encryption processing

unit" in line 6. It has been held that the recitation that "to be *__capable of__*" performing a function

is not a positive limitation but only requires the ability to so perform. It does not constitute a

limitation in any patentable sense (*__In re Hutchison__*, 69 USPQ 138). This renders the claim

indefinite because it unclear as to whether "to be *capable of* identifying which encryption

processing unit" actually identifying or merely capable of identifying which encryption

processing unit.

  Claim 12 recites the limitation "said dummy encryption processing units" in line 10.

There is insufficient antecedent basis for this limitation in the claim.

  Claim 18 recites the limitation "to be *capable of* identifying which encryption

processing unit" in line 5. It has been held that the recitation that "to be *capable of*" performing

a function is not a positive limitation but only requires the ability to so perform. It does not

constitute a limitation in any patentable sense (*In re Hutchison*, 69 USPQ 138). This renders

the claim indefinite because it unclear as to whether "to be *capable of* identifying which

encryption processing unit" actually identifying or merely capable of identifying which

encryption processing unit.

  Claims 2-6, 8, 10, 12-16, 18, and 20 are dependent on either claims 1, 9 11, or 19, and

therefore inherit the 35 U.S.C 112 second paragraph issues of the independent claims.

  The Examiner kindly requests the Applicant to point out with specificity (i.e. column and

line) in the specification where it describes/supports the aforementioned limitation.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or
> any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and
> requirements of this title.

Claims 1-6, 8-16, and 18-20 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject mater.

     Claims 1 and 9, Although the preamble of the claim recites "an encryption processing apparatus", the body of the claim does not positively recite any elements of hardware. The body of the claim includes the following units: *"a control section"* and *"an encryption processing section"*. In light of the paragraph [0143] and [0153-0154] of the original publication specification, the control section and the encryption processing section are implemented in software. In addition, in light of claim 21 and claim 22, all the steps of *"dividing an original encryption processing sequence"* and *"performing an encryption process"* are performed by software; it is clear that said sections are implemented in software, which is non-statutory subject matter. Therefore, the claims are directed to non-statutory subject matter.

     Claims 2-6, 8 and 10 are rejected with the same reason above.

Regarding to claims 11 and 19, the claims invention are not directed to eligible subject matter under 35 U.S.C § 101 in view of *In re Bilski*, 88 USPQ 2d 1385 CAFC (2008*)*. While the claims recite a series of steps or acts to be performed, a statutory "process" under 35 U.S.C § 101 process must (1) be tied to a particular machine or (2) transform underlying subject matter (such as an article or materials) to a different state or thing (See *In re Bilski*, 88 USPQ 2d 1385 CAFC (2008*)*; see also *Diamond v. Diehr*, 450 U.S. 175, 184 (1981*); Parker v. Flook*, 437 U.S. 584, 588 n.9 (1978*); Gottschalk v. Benson*, 409 U.S. 63, 70 (1972*); Cochrane v. Deener*, 94 U.S. 780,787-88 (1876)); The instant claims are neither positively tied to a particular machine that

accomplishes the claimed method steps nor transform underlying subject matter. The method

claimed including steps of *"dividing an original encryption processing sequence"*, *"setting a*

mixed encryption processing sequence", and *"performing an encryption process"* is broad

enough that the claim could be completely performed mentally, verbally or without a machine

nor is any transformation apparent; Therefore, the claimed invention is directed to non-statutory

subject matter.

     Claims 12-16, 18, and 20 are rejected with the same reason above.

                   Claim Rejections - 35 USC § 103

     The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

Claims 1-5, 9-15, 19, and 20-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Bruce Schneier, "Applied Cryptography", 2nd edition, John Wiley & Son, pg. 265-279, pg. 357-

263, 1996 in view of **Bo Lin et al.** (GB 2 345 229 A).

<u>**As per claims 11, 1, 21:**</u>

     Claim 11:

     Schneier teaches an encryption processing method for performing a data encryption

process, said encryption processing method comprising:

(a) dividing an original encryption processing sequence into a plurality of groups composed of one or more encryption processing units **[Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs; each column of the outer CBC is functioned as a triple DES]**, each group being a separate and independent encryption process for encrypting an input data, where the input data to be encrypted for one of the groups is different and generated independently relative to the input data to be encrypted for another one of the groups **[Schneier: pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs; each column of the outer CBC is functioned as a triple DES]**;

(b) setting a mixed encryption processing sequence by mixing processing sequences of encryption processing units of the plurality of groups with each other **[Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs; each column of the outer CBC is functioned as a triple DES; Mixing processing sequence of encryption processing in triple-DES Cipher Block Chaining encryption]** [[by inserting at least one encryption processing unit from one of the groups between encryption processing units from another one of the groups]] so that performance of at least one encryption processing unit from one of the groups is performed at a time between

performance of encryption processing units from another one of the groups and under a condition

in which a processing sequence of the encryption processing units, set in said dividing, within

each group is fixed [**Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it**

applies the same combination of technique on the plaintext block 16 times (See Figure

12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode;

triple-DES Cipher Block Chaining encryption is build on 3 DESs; Inner CBC and outer

CBC modes; Each triple-DES is fixed]; and

(c) performing an encryption process in accordance with the mixed encryption processing

sequence set in said setting [**Schneier: pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple**

encryption in CBC mode; Triple-DES Cipher Block Chaining encryption is build on 3

DES; Mixing processing sequence of encryption processing in triple-DES Cipher Block

Chaining (TCBC) encryption. The TCBC includes a triple-DES encryption process].

Schneier does not explicitly disclose [[by inserting at least one encryption processing unit

from one of the groups between encryption processing units from another one of the groups]].

However, Lin teaches encryption system resists differential power analysis attacks

wherein inserting at least one encryption processing unit from one of the groups between

encryption processing units from another one of the groups [**Lin: pg. 11; Insert "dummy" S**

block look-ups in to the DES routine, lines 10-28].

Thus, it would have been obvious to the person of ordinary skill in the art at the time the

invention was made to combine the encryption processing method of Schneier by including the

teaching of Lin because it would perform the DES operation and the benefit gained in DPA

attack resistance [**Lin: pg. 11, lines 18-19**].

Claims 1 and 21 are essentially the same as claim 11 except that they set forth the
claimed invention as an apparatus / a computer readable storage medium rather than a method
and rejected under the same reasons as applied above.

As per claims 12, 2:

Claim 12:

The combination of Schneier and Lin teach the subject matter as described above.

Schneier further teaches an encryption processing method according to Claim 11,
wherein each group includes a triple-DES encryption process **[Schneier: pg. 270-278; DES is a
block cipher. DES has 16 rounds; it applies the same combination of technique on the
plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1,
Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on
3 DESs; each column of the outer CBC is functioned as a triple DES].**

Lin further teaches, setting a dummy encryption processing unit that performs the dummy
encryption process in at least one of the groups, and setting the mixed encryption processing
sequence by mixing the encryption processing units of a plurality of groups containing said
dummy encryption processing units **[Lin: abstract, pg. 11, lines 10-28; "Another technique
which could be used to improve resistance to attacks is to *insert* "dummy" operation to
confuse analysis of a power signature... The number of dummy look-ups performed can be
chosen to optimize the time it takes to perform the DES operation and the benefit gained in
DPA attack resistance ...". It would have been obvious for setting the number of single-**

DES processes of dummies to be set to a multiple of 3 corresponding to the triple DES

because each number of single-DES is set to 1].

       dividing includes setting a dummy single-DES process as a dummy encryption process

that is unnecessary for the original encryption processing sequence in at least one of said groups,

and setting the number of single-DES processes of dummies to be set to a multiple of 3 **[Lin:**

abstract, pg. 11, lines 10-28; "Another technique which could be used to improve resistance

to attacks is to insert "dummy" operation to confuse analysis of a power signature... The

number of dummy look-ups performed can be chosen to optimize the time it takes to

perform the DES operation and the benefit gained in DPA attack resistance ...". It would

have been obvious for setting the number of single-DES processes of dummies to be set to a

multiple of 3 corresponding to the triple DES because each number of single-DES is set to

1].

       Claim 2 is essentially the same as claim 12 except that they set forth the claimed

invention as an apparatus rather than a method and rejected under the same reasons as applied

above.

As per claim 13, 3:

  Claim 13:

       The combination of Schneier and Lin teache the subject matter as described above.

       Schneier further teaches an encryption processing method according to Claim 11,

wherein said dividing determines a group of sequences, which can be performed independently

of each other, within the original encryption processing sequence to be divided in a process of

division into the plurality of groups, and performs a process for setting a group of divisions in

which each of the sequences in the group of sequences can be performed independently as a unit

[Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same

combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361,

15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher

Block Chaining encryption is build on 3 DES; page 272, figure 12.2 One round of DES;

Each S-box independently performs an encryption processing as a unit].

   Claim 3 is essentially the same as claim 13 except that they set forth the claimed invention as

an apparatus rather than a method and rejected under the same reasons as applied above.

As per claims 14, 4:

   Claim 14:

       The combination of Schneier and Lin teach the subject matter as described above.

        Schneier further teaches an encryption processing method according to Claim 11,

wherein each of said encryption processing units is a single-DES encryption process,

       (a) said dividing divides the original encryption processing sequence containing one or

more single-DES encryption processes into a plurality of groups composed of one or more

single-DES encryption processes **[Schneier : pg. 270-278; DES is a block cipher. DES has 16**

rounds; it applies the same combination of technique on the plaintext block 16 times (See

Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC

mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs], and

(b) said setting sets one mixed encryption processing sequence by mixing the single-DES encryption processing units contained in each group by mutual replacement of the single-DES encryption processing units of each set group under the condition in which the processing sequence within each set group is fixed **[Schneier : pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; Triple-DES Cipher Block Chaining encryption is build on 3 DES; Mixing processing sequence of encryption processing in triple-DES Cipher Block Chaining encryption. Each triple-DES is fixed]**.

Claim 4 is essentially the same as claim 14 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

As per claims 15, 5:

Claim 15:

The combination of Schneier and Lin teach the subject matter as described above.

Schneier further teaches an encryption processing method according to Claim 11, wherein said dividing performs a process for dividing the encryption processing sequence into a plurality of groups composed of one or more encryption processing units with a single-DES encryption process which forms a triple-DES encryption process being an encryption processing unit **[Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher**

Block Chaining encryption is build on 3 DESs].

  Claim 5 is essentially the same as claim 15 except that they set forth the claimed invention as
an apparatus rather than a method and rejected under the same reasons as applied above.

<u>**As per claims 19, 9, 22:**</u>

   Claim 19:

     Schneier teaches an encryption processing method for performing a data encryption process,
said encryption processing method comprising:

        (a) dividing an original encryption processing sequence, into a plurality of groups which
include one or more encryption processing units **[Schneier: pg. 270-278; DES is a block
cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext
block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple
encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3
DESs]**, each group being a separate and independent encryption process for encrypting an input
data, where the input data to be encrypted for one of the groups is different and generated
independently relative to the input data to be encrypted for the another one of the groups
**[Schneier: pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC
mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs; each column of
the outer CBC is functioned as a triple DES]**,

        (b) setting a mixed encryption processing sequence **[Schneier: pg. 270-278; DES is a
block cipher. DES has 16 rounds; it applies the same combination of technique on the**

plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs; each column of the outer CBC is functioned as a triple DES; Mixing processing sequence of encryption processing in triple-DES Cipher Block Chaining encryption] [[by adding dummy encryption processing units as encryption processing units to at least one of the groups, the dummy encryption processing units performing dummy encryption processes that are unnecessary for the original processing sequence]] and by mixing processing sequences of the encryption processing units of the plurality of groups with each other [[by inserting at least one encryption processing unit from one of the groups between encryption processing units from another one of the groups]] so that performance of at least one encryption processing unit from one of the groups is performed at a time between performance of encryption processing units from another one of the groups **[Schneier: pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs; Inner CBC and outer CBC modes; Each triple-DES is fixed];** and

   (c) performing an encryption process in accordance with said mixed encryption processing sequence **[Schneier : pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; Triple-DES Cipher Block Chaining encryption is build on 3 DES; Mixing processing sequence of encryption processing in triple-DES Cipher Block Chaining (TCBC) encryption. In the TCBC includes a triple-DES encryption process]**.

Scheier does not explicitly disclose dummy encryption processing units performing
/dummy encryption processes that are unnecessary for the original processing sequence, inserting
at least one encryption processing unit from one of the groups between encryption processing
units from another one of the groups.

However, Lin teaches encryption system resists differential power analysis attacks
wherein dummy encryption processing units performing dummy encryption processes that are
unnecessary for the original processing sequence, inserting at least one encryption processing
unit from one of the groups between encryption processing units from another one of the
groups.[**Lin: abstract, pg. 11, lines 10-28; "Another technique which could be used to
improve resistance to attacks is *to insert* "dummy" operation to confuse analysis of a power
signature... The number of dummy look-ups performed can be chosen to optimize the time
it takes to perform the DES operation and the benefit gained in DPA attack resistance..."].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the
invention was made to combine the encryption processing method of Schneier by including the
teaching of Lin because it would perform the DES operation and the benefit gained in DPA
attack resistance [**Lin: pg. 11, lines 18-19].**

  Claims 9 and 22 are essentially the same as claim 19 except that they set forth the claimed
invention as an apparatus / a computer readable storage medium rather than a method and
rejected under the same reasons as applied above.

As per claims 20, 10:

Claim 20:

Schneier and Lin teach the subject matter as described above.

Schneier further teaches an encryption processing, wherein an encryption processing unit contained in said original encryption processing sequence is a single-DES encryption process **[Schneier : pg. 270-278; DES is a block cipher. DES has 16 rounds; it applies the same combination of technique on the plaintext block 16 times (See Figure 12.1); pg. 358-361, 15.2 Triple encryption; figure 15.1, Triple encryption in CBC mode; triple-DES Cipher Block Chaining encryption is build on 3 DESs],**

Lin further teaches said dummy encryption processes as a single-DES encryption process **[Lin: abstract, pg. 11, lines 10-28"; "Another technique which could be used to improve resistance to attacks is to insert "dummy" operation to confuse analysis of a power signature... The number of dummy look-ups performed can be chosen to optimize the time it takes to perform the DES operation and the benefit gained in DPA attack resistance..."],** and

Schneier and Lin do not explicitly disclose wherein said dividing includes setting the number of dummy encryption processes to a multiple of 3.

It would have been obvious for setting the number of single-DES processes of dummies to be set to a multiple of 3 corresponding to the triple DES because each number of single-DES is set to 1.

Claim 10 is essentially the same as claim 20 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

Claims 6 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bruce Schneier,** "Applied Cryptography", 2nd edition, John Wiley & Son, pg. 265-279, pg. 357-263, 1996 in view of **Bo Lin et al.** (GB 2 345 229 A) further in view of **Kocher et al.** (US 2001/0053220 A1).

<u>As per claims 16, 6:</u>

Claim 16:

The combination of Schneier and Lin teach the subject matter as described above.

Schneier and Lin do not explicitly disclose in details a random-number generation process as a process including a conversion process by three single-DES processes and setting the three single-DES processes as a random- number generation process in one of the groups.

However, Kocher teaches a random-number generation process as a process including a conversion process by three single-DES processes and setting the three single-DES processes as a random-number generation process in one of the groups **[Kocher: par. [0006]; "triple DES (a cipher constructed using three applications of Data Encryption Standard using different keys) can resist all feasible cryptanalytic attacks, provided that attackers only have access to the standard inputs to and outputs from the protocol"; par. [0008], lines 6-8; a key management devices introduce randomness].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the encryption processing method of Schneier and Lin by

including the teaching of Kocher because it would provide unpredictability into their internal
state [**Kocher, par. [008]**].

       Claim 6 is essentially the same as claim 16 except that they set forth the claimed
invention as an apparatus rather than a method and rejected under the same reasons as applied
above

Claims 8 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Bruce
Schneier**, "Applied Cryptography", 2nd edition, John Wiley & Son, pg. 265-279, pg. 357-263,
1996 in view of **Bo Lin et al.** (GB 2 345 229 A) further in view of **Kaminaga et al** (US
2002/0124179 A1).

As per claims 18, 8:
    Claim 18:
    The combination of Schneier and Lin teach the subject matter as described above.
    Schneier and Lin do not explicitly disclose in details storing processing results in a memory
for storing processing results of the encryption processing units which form the mixed
encryption processing sequence in such a manner as to be capable of identifying which
encryption processing unit the processing results are obtained from.
       However, Kaminaga teaches storing processing results in a memory for storing
processing results of the encryption processing units which form the mixed encryption
processing sequence in such a manner as to be capable of identifying which encryption

processing unit the processing results are obtained from **[Kaminaga: abstract, par. [0039], lines 7-10; "processed by an encryption process (step 503). The result Z obtained in the process performed in step 503 is stored on a RAM (step 504)"].**

Thus, it would have been obvious to the person of ordinary skill in the art at the time the invention was made to combine the encryption processing method of Schneier and Lin by including the teaching of Kaminaga because it would detect an erroneous operation during encryption processing is that before the output of the encrypted result, the ciphertext result, the ciphertext is again decrypted to a plaintext and compared with the original text, and when they are identical to each other, the ciphertext is output and when they are different, the result of the encryption-process is not output to the external device **[Kaminaga, par. [0014]].**

Claim 8 is essentially the same as claim 18 except that they set forth the claimed invention as an apparatus rather than a method and rejected under the same reasons as applied above.

Conclusion

The examiner requests, in response to this Office action, support be shown for language added to any original claims on amendment and any new claims. That is, indicate support for newly added claim language by specifically pointing to page(s) and line number(s) in the specification and/or drawing figure(s). This will assist the examiner in prosecuting the application. Failure to show support can result in a non-compliant response.

When responding to this office action, Applicant is advised that if Applicant traverses an obviousness rejection under 35 U.S.C. 103, a reasoned statement must be included explaining why the Applicant believes the Office has erred substantively as to the factual findings or the conclusion of obviousness See 37 CFR 1.111(b).

Additionally Applicant is further advised to clearly point out the patentable novelty which he or she thinks the claims present, in view of the state of the art disclosed by the references cited or the objections made. He or she must also show how the amendments avoid such references or objections See 37 CFR 1.111(c).

The prior arts made of record and not relied upon are considered pertinent to applicant's disclosure.

US 6839847 B1 to Ohki; Masaru et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Canh Le whose telephone number is 571-270-1380. The examiner can normally be reached on Monday to Friday 7:30AM to 5:00PM other Friday off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Orgad Edan can be reached on 571-272-7884. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would

like assistance from a USPTO Customer Service Representative or access to the automated

information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Canh Le/

Examiner, Art Unit 2439

August 6, 2009

/Edan Orgad/
Supervisory Patent Examiner, Art Unit 2439